CHABAUTY–COLEMAN EXPERIMENTS FOR GENUS 3 HYPERELLIPTIC CURVES

JENNIFER S. BALAKRISHNAN, FRANCESCA BIANCHI, VICTORIA CANTORAL-FARFÁN, MIRELA ÇIPERIANI, AND ANASTASSIA ETROPOLSKI

Abstract. We describe a computation of rational points on genus 3 hyperelliptic curves C defined over $\mathbb{Q}$ whose Jacobians have Mordell–Weil rank 1. Using the method of Chabauty and Coleman, we present and implement an algorithm in `Sage` to compute the zero locus of two Coleman integrals and analyze the finite set of points cut out by the vanishing of these integrals. We run the algorithm on approximately 17,000 curves from a forthcoming database of genus 3 hyperelliptic curves and discuss some interesting examples where the zero set includes global points not found in $C(\mathbb{Q})$.

1. Introduction

Let C be a non-singular curve over $\mathbb{Q}$ (or more generally, a number field K) of genus g. In the case where $g = 0$ or $g = 1$, C has extra structure given by the fact that if $C(\mathbb{Q})$ is non-empty, then C is rational (if $g = 0$) or C is an elliptic curve (if $g = 1$). In these cases, computing the set of rational points is either trivial by the Hasse Principle, or highly non-trivial in the case of elliptic curves. In the latter case the rational points form a finitely generated abelian group, and methods specific to this case exist for computing upper bounds on the rank of $C(\mathbb{Q})$, and the possibilities for the torsion subgroup of $C(\mathbb{Q})$ are completely understood by the work of Mazur [Maz77, Theorem 8].

On the other hand, if $g \geq 2$, then C is of general type, and the Mordell conjecture, proved by Faltings in 1983 [Fal83], implies that $C(\mathbb{Q})$ is finite. Our main motivation is to compute $C(\mathbb{Q})$ explicitly in this case. We will focus our attention on hyperelliptic curves of genus 3 such that the group of rational points of the Jacobian of C has Mordell–Weil rank $r = 1$. This falls into the special case where $r < g$ which was considered by Chabauty in 1941 [Cha41], and techniques developed by Coleman in the 1980s allow us to use p-adic integration to bound, and often, in practice, explicitly compute, the set of rational points [Col85b, Col85a].

In addition to these methods, we will also use the algorithm of Balakrishnan, Bradshaw, and Kedlaya [BBK10] and its implementation in `Sage` [S+17] to explicitly compute the relevant Coleman integrals by computing analytic continuation of Frobenius on curves. Nonetheless, we note that the algorithms presented in this article (see Section 3) have not been implemented previously by other authors or carried out on a large collection of curves. (See, however, [BS08] for related work in genus 2.) Our code is available at [BBCF+].

We consider the case of genus 3 hyperelliptic curves for two reasons:

(1) When $g = 3$, we can impose the condition that $0 < r < g - 1$, i.e. $r = 1$, which, by a dimension argument, makes the method more effective. Indeed, in this case, the set

Date: May 8, 2018.

$C(\mathbb{Q})$ is contained in the intersection of the zero sets of the integrals of two linearly independent regular 1-forms on the base-change of C to $\mathbb{Q}_p$, where p is any odd prime of good reduction.

(2) When $g = 2$, the Jacobian of C is a surface, and its geometry and arithmetic is better understood. In particular, methods developed by Cassels and Flynn have been implemented by Stoll in `Magma` to make the computations needed much more efficient. More precisely, in this case, one can simplify the algorithm further by working with the quotient of the Jacobian by $\langle \pm 1 \rangle$, which is a quartic surface in $\mathbb{P}^3$, known as the Kummer surface. In order to make the search of rational points more effective, the Chabauty method can also be combined with the Mordell–Weil sieve, which uses information at different primes (see also [BS10]).

We begin with an overview of the Chabauty–Coleman method and explicit Coleman integration in Section 2. In Section 3, we present an algorithm to find a finite set of p-adic points containing the rational points of a hyperelliptic curve $C/\mathbb{Q}$ of genus 3, which admits an odd model, and whose Jacobian J has rank 1. We fix a prime p and work under the assumption that we know a $\mathbb{Q}$-rational point whose image in the Jacobian has infinite order (here the embedding of C into J is via the base-point ∞). Besides $\mathbb{Q}$-rational points, the output will include all points in $C(\mathbb{Q}_p)$ which are in the pre-image of the p-adic closure of $J(\mathbb{Q})$ in $J(\mathbb{Q}_p)$.

We then proceed to run our code on a list of relevant curves taken from the forthcoming database of genus 3 hyperelliptic curves [BPSS]. Our list consists of 16,977 curves, and we separately do a point search in `Magma` to find all $\mathbb{Q}$-rational points whose x-coordinates with respect to a fixed integral affine model have naive height at most 10^5 (cf. Section 4). Our Chabauty–Coleman computations then show that there are no $\mathbb{Q}$-rational points of larger height on any of these curves.

In some cases, our algorithm outputs points in $C(\mathbb{Q}_p)\backslash C(\mathbb{Q})$. Besides $\mathbb{Q}_p$-rational (but non-$\mathbb{Q}$-rational) Weierstrass points, on 75 curves we find that the local point is the localization of a point $P \in C(K)$ where K is a quadratic field in which the prime p splits. In all these cases, we are able to explain why these points appear in the zero locus that we are studying. The following three scenarios occur, and we discuss representative examples of each in Section 4:

- It may happen that $[P - \infty]$ is a torsion point in the Jacobian (see Example 4.1). In this case, the integral of any 1-form would vanish between ∞ and P.
- As in Example 4.2, it may happen that some multiple of the image of $[P - \infty]$ in the Jacobian actually belongs to $J(\mathbb{Q})$: the vanishing here follows by linearity in the endpoints of integration.
- The Jacobian J may decompose over $\mathbb{Q}$ as a product of an elliptic curve and an abelian surface. Then if the subgroup H generated by $J(\mathbb{Q})$ and the point $[P - \infty]$ comes from the elliptic curve, the dimension of the p-adic closure of H in $J(\mathbb{Q}_p)$ must be equal to 1, even if $[P - \infty]$ is a point of infinite order (see Example 4.3).

Acknowledgements. The first author is supported in part by NSF grant DMS-1702196, the Clare Boothe Luce Professorship (Henry Luce Foundation), and Simons Foundation grant #550023. The second author is supported by EPSRC and by Balliol College through a Balliol Dervorguilla scholarship. The third author was supported by a Conacyt fellowship. The fourth author is supported by NSF grant DMS-1352598.

This project began at "WIN4: Women in Numbers 4," and we are grateful to the conference organizers for facilitating this collaboration. We further acknowledge the hospitality and support provided by the Banff International Research Station. We thank the Simons Collaboration on Arithmetic Geometry, Number Theory, and Computation for providing computational resources, and we are grateful to Bjorn Poonen, Andrew Sutherland, and Raymond van Bommel for helpful conversations.

2. The Chabauty–Coleman method and Coleman integration

In this section, we review the Chabauty–Coleman method, used to compute rational points in our main algorithm. For further details, see Section 3. We also give a brief overview of explicit Coleman integration on hyperelliptic curves.

2.1. Chabauty–Coleman method.

Let C be a smooth, projective curve over the rationals of genus at least 2. By the work of Faltings [Fal83], we know $C(\mathbb{Q})$ to be finite, but Faltings' proof does not explicitly yield the set $C(\mathbb{Q})$. However, before the work of Faltings, Chabauty considered the following set-up. Let p be a prime and $P \in C(\mathbb{Q}_p)$. Consider the embedding

$$\begin{aligned} \iota_P \colon C &\hookrightarrow J \\ Q &\mapsto [Q - P]. \end{aligned}$$

Then let $\overline{J(\mathbb{Q})}$ denote the p-adic closure of $J(\mathbb{Q})$ and define

$$C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})} := \iota_P(C(\mathbb{Q}_p)) \cap \overline{J(\mathbb{Q})}.$$

Chabauty proved the following case of Mordell's conjecture:

Theorem 2.1 ([Cha41])**.** *Let $C/\mathbb{Q}$ be a curve of genus $g \geq 2$ such that the Mordell–Weil rank of the Jacobian J of C over $\mathbb{Q}$ is less than g, and let p be a prime. Then $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ is finite.*

Chabauty's result was later re-interpreted and made effective by Coleman, who showed the following:

Theorem 2.2 ([Col85a])**.** *Let C be as above and suppose that p is a prime of good reduction for C. If $p > 2g$, then*

$$\#C(\mathbb{Q}) \leq \#C(\mathbb{F}_p) + 2g - 2.$$

To obtain an explicit upper bound on the size of $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$, and hence $C(\mathbb{Q})$, Coleman used his theory of p-adic integration on curves to construct p-adic integrals of 1-forms on $J(\mathbb{Q}_p)$ that vanish on $J(\mathbb{Q})$ and restrict them to $C(\mathbb{Q}_p)$. Here, we follow the exposition in [Wet97] in defining the Coleman integral.

Let $\omega_J \in H^0(J_{\mathbb{Q}_p}, \Omega^1)$, and λ_{ω_J} be the unique homomorphism $\lambda_{\omega_J} \colon J(\mathbb{Q}_p) \to \mathbb{Q}_p$ such that $d(\lambda_{\omega_J}) = \omega_J$. Consider the map induced by ι_P

$$\iota^* \colon H^0(J_{\mathbb{Q}_p}, \Omega^1) \to H^0(C_{\mathbb{Q}_p}, \Omega^1).$$

Observe that ι^* is an isomorphism of vector spaces which is independent of the choice of $P \in C(\mathbb{Q}_p)$ [Mil86, Proposition 2.2].

Define $\omega := \iota^*(\omega_J)$ to be the corresponding differential on C. On the Jacobian we have the natural pairing

$$\lambda\colon H^0(J_{\mathbb{Q}_p}, \Omega^1) \times J(\mathbb{Q}_p) \to \mathbb{Q}_p$$
$$(\omega_J, R) \mapsto \lambda_{\omega_J}(R) := \int_0^R \omega_J.$$

Note that since λ_{ω_J} is a homomorphism, it vanishes on $J(\mathbb{Q}_p)_{\text{tors}}$. Now given $P, Q \in C(\mathbb{Q}_p)$ we define

$$\int_P^Q \omega := \int_0^{[Q-P]} \omega_J,$$

hence for a fixed point $P \in C(\mathbb{Q}_p)$ and $\omega \in H^0(C_{\mathbb{Q}_p}, \Omega^1)$ we get a function $\lambda_{\omega,P}\colon C(\mathbb{Q}_p) \to \mathbb{Q}_p$ with

$$\lambda_{\omega,P}(Q) := \int_P^Q \omega = \int_0^{[Q-P]} \omega_J = \lambda_{\omega_J}([Q-P]).$$

We now restrict to the case where $g = g(C) = 3$ and $r = \operatorname{rank} J(\mathbb{Q}) = 1$, in which case $g - r = 2$. The exposition below can be generalized whenever $r < g$. Let

$$\operatorname{Ann}(J(\mathbb{Q})) := \left\{ \omega_J \in H^0(J_{\mathbb{Q}_p}, \Omega^1) : \lambda_{\omega_J}(R) = \int_0^R \omega_J = 0 \text{ for all } R \in J(\mathbb{Q}) \right\}.$$

This is a 2-dimensional $\mathbb{Q}_p$-vector space; hence there exist two linearly independent differentials $\alpha_J, \beta_J \in H^0(J_{\mathbb{Q}_p}, \Omega^1)$ such that

$$\lambda_{\alpha_J}(R) = \lambda_{\beta_J}(R) = 0 \quad \text{for all } R \in J(\mathbb{Q}).$$

Let D be a $\mathbb{Q}$-rational divisor on C of degree r, and consider the map $\iota_D\colon C \to J$ such that $Q \mapsto [rQ - D]$. Define

$$\lambda_{\omega,D}(Q) := \lambda_{\omega_J} \circ \iota_D(Q) = \lambda_{\omega_J}(rQ - D).$$

Consider the set

$$\begin{aligned} Z &:= \{Q \in C(\mathbb{Q}_p) : \lambda_{\omega,D}(Q) = 0 \text{ for all } \omega \in \operatorname{Ann}(J(\mathbb{Q}))\} \\ &= \ker(\lambda_{\alpha,D}) \cap \ker(\lambda_{\beta,D}). \end{aligned} \tag{2.1}$$

While a priori we have defined Z in terms of D, it is actually independent of the choice of D, and $C(\mathbb{Q}) \subseteq Z$ [Wet97, §1.6].

The above discussion indicates how we would handle the case when our hyperelliptic curve has an even degree model. However, since we restrict our attention to hyperelliptic curves C with an odd degree model, we are guaranteed a rational point $\infty \in C(\mathbb{Q})$ and we use $D = \infty$. Hence, we have two $\mathbb{Q}_p$-valued functions $\lambda_{\alpha,\infty}, \lambda_{\beta,\infty}$ on $C(\mathbb{Q}_p)$ whose common zeros capture the rational points of C.

2.2. **Computing Coleman integrals.** In order to compute Z, we need a way to evaluate $\int_P^Q \omega$ for an arbitrary $\omega \in H^0(C_{\mathbb{Q}_p}, \Omega^1)$ and arbitrary $P, Q \in C(\mathbb{Q}_p)$. Suppose that p is a prime of good reduction for C and let $\overline{C}$ be the reduction of C modulo p, i.e. the special fiber of a minimal regular proper model of C over $\mathbb{Z}_p$. Then there exists a natural reduction map $C(\mathbb{Q}_p) \to \overline{C}(\mathbb{F}_p)$. Define a residue disk to be a fiber of the reduction map. To compute $\int_P^Q \omega$, we now consider two cases: either P and Q lie in the same residue disk, or they do not.

2.2.1. *Coleman integral within a residue disk.* Let $P \in C(\mathbb{Q}_p)$. By a local coordinate for P we mean a rational function $t \in \mathbb{Q}_p(C)$ such that

(1) t is a uniformizer at P; and
(2) the reduction of t to a rational function for $\overline{C}$ is a uniformizer at $\overline{P}$.

Hence, a local coordinate t at P establishes a bijection

$$\begin{aligned} p\mathbb{Z}_p &\leftrightarrow \{Q \in C(\mathbb{Q}_p) : \overline{Q} = \overline{P}\} \\ t &\leftrightarrow (x(t), y(t)), \end{aligned}$$

where $x(t), y(t)$ are Laurent series and $(x(0), y(0)) = P$.

Suppose now that $\omega \in H^0(C_{\mathbb{Q}_p}, \Omega^1)$ is not identically zero modulo p. We will often use the fact that the expansion of ω in terms of t has the form $w(t)dt$, for some $w(t) \in \mathbb{Z}_p[[t]]$ converging on the entire residue disk. Hence, if $\overline{Q} = \overline{P}$, we can compute $\int_P^Q \omega$ by formally integrating a power series in the local coordinate t ([Wet97, Lemma 7.2]). Such definite integrals are referred to as tiny integrals.

A local coordinate at a given point $P \in C(\mathbb{Q}_p)$ can be found using [Bal15, Algorithms 2-4]. In particular,

(1) If $y(\overline{P}) \neq 0$, then $x(t) = t + x(P)$ and $y(t)$ is the unique solution to $y^2 = f(x(t))$ such that $y(0) = y(P)$.
(2) If $y(\overline{P}) = 0$ and $\overline{P} \neq \overline{\infty}$, then $y(t) = t + y(P)$ and $x(t)$ is the unique solution to $f(x) = y(t)^2$ such that $x(0) = x(P)$.
(3) If $\overline{P} = \overline{\infty}$, one first finds $x(t) = t^{-2} + O(1)$ by solving $f(x) = \frac{x^6}{t^2}$. Then $y(t) = \frac{x(t)^3}{t}$.

In practice, in all three cases one can explicitly compute $(x(t), y(t))$ up to arbitrary p-adic and t-adic precision by Newton's method.

2.2.2. *Coleman integral between different residue disks.* In our intended application of computing rational points, we will fix a basepoint as one endpoint of integration and consider the various Coleman integrals given by varying the other endpoint of integration over all residue disks. This makes it essential that the tiny integrals constructed in the previous section are consistent across the set of residue disks: in other words, we need a notion of analytic continuation between different residue disks.

Coleman solved this problem by using Frobenius to write down a unique "path" between different residue disks and presented a theory of p-adic line integration on curves [Col85b] satisfying a number of natural properties, among them linearity in the integrand, additivity in endpoints, change of variables via rigid analytic maps (e.g., Frobenius), and the fundamental theorem of calculus. This was made algorithmic in [BBK10] for *hyperelliptic* curves by solving a linear system induced by the action of Frobenius on Monsky-Washnitzer cohomology, with an implementation available in `Sage`.

The upshot is that given two points $P, Q \in C(\mathbb{Q}_p)$, one can compute the definite Coleman integral from P to Q as $\int_P^Q \omega$ directly via [BBK10], as well as the Coleman integral from P to the residue disk of Q, by further computing a local coordinate t_Q at Q (such that $t_Q|_{t=0} = Q$), which gives:

$$\int_P^{t_Q} \omega = \int_P^Q \omega + \int_Q^{t_Q} \omega = \int_P^Q \omega + \int_0^t \omega,$$

where $\int_P^Q \omega$ now plays the role of the constant of integration between different residue disks.

3. The algorithm

We now specialize to our case of interest, where C is a genus 3 hyperelliptic curve given by an odd degree model, i.e.,

$$C\colon y^2 = F(x)$$

where $F(x) \in \mathbb{Q}[x]$ is monic of degree 7. We will further assume that the Jacobian J of C has Mordell–Weil rank 1 over $\mathbb{Q}$. Finally, we will assume that we have computed a point $P_0 \in C(\mathbb{Q})$ with the property that $[P_0 - \infty]$ is of infinite order in $J(\mathbb{Q})$. (This last assumption is straightforward to remove.)

Fix an odd prime p of good reduction for C, denote by $\overline{C}$ the base change of C to $\mathbb{F}_p$ and let $C(\mathbb{Q})_{\text{known}}$ denote a list of known points in $C(\mathbb{Q})$. Given this input, the algorithm in this section returns the set Z of common zeros of $\lambda_{\alpha,\infty}$ and $\lambda_{\beta,\infty}$, as defined in Section 2.1, excluding the known rational points $C(\mathbb{Q})_{\text{known}}$.

3.1. **Upper Bounds in Residue Disks.** Define $\omega_i = (x^i/2y)dx$ for $i \in \{0,1,2\}$. These differentials form a basis for $H^0(C_{\mathbb{Q}_p}, \Omega^1)$. Let α and β be 1-forms in $H^0(C_{\mathbb{Q}_p}, \Omega^1)$ such that α_J and β_J form a basis for $\mathrm{Ann}(J(\mathbb{Q}))$ and such that α and β are not identically zero modulo p. We may assume that we are in one of the following two situations:

(1) $\alpha = \omega_0$ and β is a $\mathbb{Z}_p$-linear combination of ω_1 and ω_2, or
(2) α is a $\mathbb{Z}_p$-linear combination of ω_0 and ω_1 and β is a $\mathbb{Z}_p$-linear combination of ω_0 and ω_2.

Let $f'(t)$ be the local expansion of α or β in the residue disk of a point $\overline{Q} \in \overline{C}(\mathbb{F}_p)$. Ultimately we want to compute the zeros of a particular antiderivative $f(t)$ lying in $p\mathbb{Z}_p$ up to a desired p-adic precision. In certain cases, we will be able to avoid this calculation by instead obtaining an upper bound for the number of zeros of $f(t)$ in $p\mathbb{Z}_p$ which we know to be sharp. To do this, we use the theory of Newton polygons for p-adic power series (see, e.g., [Kob84, IV.4]).

Given $f(t) \in \mathbb{Q}_p[[t]]$ such that $f'(t) \in \mathbb{Z}_p[[t]]$, let $\overline{f'}(t) = f'(t) \pmod p$ and define

$$m_f := \mathrm{ord}_{t=0}\overline{f'}(t). \tag{3.1}$$

The following result is [MP12, Lemma 5.1] and can be viewed as a corollary of the p-adic Weierstrass Preparation Theorem [Kob84, Ch. IV, §4, Theorem 14].

Lemma 3.1. *Let $f(t) \in \mathbb{Q}_p[[t]]$ such that $f'(t) \in \mathbb{Z}_p[[t]]$. If $m_f < p-2$, then the number of roots of f in $p\mathbb{Z}_p$ is less than or equal to $m_f + 1$.*

Remark 3.2. Note that if $p > 2g = 6$ and $f'(t)$ is the local expansion of a regular 1-form, then the Riemann-Roch Theorem implies that $m_f \leq 4$ and hence the condition $m_f < p-2$ of Lemma 3.1 is always satisfied (cf. [MP12, Theorem 5.3]).

The following lemmas give a refinement of this result for our particular choice of f. We refer to a point of C or $\overline{C}$ as a Weierstrass point if it is fixed by the hyperelliptic involution.

Lemma 3.3. *Let $f'(t)$ be the local expansion of α or β in the residue disk of a point $\overline{Q} \in \overline{C}(\mathbb{F}_p)$. If $\overline{Q}$ is non-Weierstrass, then*

$$m_f \leq \begin{cases} 1 & \text{if } x(\overline{Q}) \neq 0, \\ 2 & \text{else.} \end{cases}$$

Moreover, the minimum of the orders of vanishing of α and β at $\overline{Q}$ is less than or equal to 1 for all non-Weierstrass $\overline{Q}$.

Proof. By construction, the differential f' is a linear combination of two of the differentials $\omega_i = (x^i/2y)dx$, $i = 0, 1, 2$, and f' is non-trivial modulo p. The assumption that $\overline{Q}$ is non-Weierstrass implies that $t = x - x(Q)$ is a local coordinate, where Q is any lift of $\overline{Q}$ to characteristic zero. Write $f' = ((Ax^i + Bx^j)/2y)dx$, where $A, B \in \mathbb{Z}_p$, $i, j \in \{0, 1, 2\}$, $i < j$. Then in local coordinates we have

$$f'(t) = \frac{A(t + x(Q))^i + B(t + x(Q))^j}{2y(t)}dt$$

where $y(t)$ has no zeros or poles in the residue disk. Since $A(t + x(Q))^i + B(t + x(Q))^j$ is a polynomial of degree less than or equal to 2 in t, the first part of the first claim is proved. Furthermore, the polynomial has a double root modulo p at $\overline{Q}$ if and only if $A \equiv 0 \bmod p$, $j = 2$, $B \not\equiv 0$, and $x(\overline{Q}) = 0$; i.e., if and only if $f' \equiv \frac{x^2}{2y}dx$ (up to rescaling) and $x(\overline{Q}) = 0$. The last statement also follows, since by construction α is a linear combination of ω_0 and ω_1 (see the beginning of §3.1). □

Proposition 3.4. *Let p be an odd prime greater than or equal to 5 of good reduction for C. Let $\overline{Q} \in \overline{C}(\mathbb{F}_p)$ be a non-Weierstrass point. Then the set*

$$\left\{ P \in C(\mathbb{Q}_p) : \overline{P} = \overline{Q} \text{ and } \int_\infty^P \alpha = \int_\infty^P \beta = 0 \right\}$$

has size less than or equal to 2.

Proof. Follows from Lemma 3.1 and Lemma 3.3. □

Lemma 3.5. *Let $f'(t)$ be the local expansion of α or β in the residue disk of the point $\overline{\infty} \in \overline{C}(\mathbb{F}_p)$. Then $m_f \in \{0, 2, 4\}$. In particular, the minimum of the orders of vanishing of α and β at $\overline{\infty}$ is less than or equal to 2.*

Proof. We may take $x(t) = t^{-2} + O(1)$, $y(t) = t^{-7} + O(t^{-5})$ (cf. [Bal15, Algorithm 4]). Then $x^i dx/2y$ has a zero of order $4 - 2i$ at $t = 0$. □

Proposition 3.6. *Let p be an odd prime greater than or equal to 5 of good reduction for C. Then the set*

$$\left\{ P \in C(\mathbb{Q}_p) : \overline{P} = \overline{\infty} \text{ and } \int_\infty^P \alpha = \int_\infty^P \beta = 0 \right\}$$

has size less than or equal to 3. In particular, there are at most two points different from the point at infinity and reducing to it modulo p in the above set.

Lemma 3.7. *Let $f'(t)$ be the local expansion of α or β in the residue disk of a point $\overline{Q} \in \overline{C}(\mathbb{F}_p)$ (with the notation of the algorithm). If $\overline{Q}$ is Weierstrass, then*

$$m_f \in \begin{cases} \{0,2\} & \text{if } x(\overline{Q}) \neq 0, \\ \{0,2,4\} & \text{else.} \end{cases}$$

Moreover, the minimum of the orders of vanishing of α and β at $\overline{Q}$ is less than or equal to 2.

Proof. In this case we may take $y = t$ and solve for x using $y^2 = F(x)$. In particular, then $x(t) = x(Q) + \frac{t^2}{F'(x(Q))} + O(t^4) \mod p$ (cf. [Bal15, Algorithm 3]). Therefore, $dx/2y$ has no zero or pole at $t = 0$, $x^i dx/2y$ has either no zero or pole or a zero of order $2i$ if $\overline{Q} = (0,0)$. Now consider

$$f'(t) = \left(A \left(x(Q) + \frac{t^2}{f'(x(Q))} + O(t^4) \right)^i + B \left(x(Q) + \frac{t^2}{f'(x(Q))} + O(t^4) \right)^j \right) u(t) dt,$$

where $u(t)$ is a unit power series and A is non-zero modulo p. For any choice of $i, j \in \{0,1,2\}$, $i < j$, it can be verified that $m_f \in \{0,2\}$ by distinguishing between the cases $x(\overline{Q}) = 0$ or $x(\overline{Q}) \neq 0$. If $A \equiv 0 \mod p$ when $i = 0$ or 1 and $j = 2$ then m equals 4 if $x(\overline{Q}) = 0$. However, by construction, α and β cannot both be of this form. □

Proposition 3.8. *Let p be an odd prime greater than or equal to 5 of good reduction for C. Let $\overline{Q} \in \overline{C}(\mathbb{F}_p)$ be a finite Weierstrass point. Then the set*

$$\left\{ P \in C(\mathbb{Q}_p) : \overline{P} = \overline{Q} \text{ and } \int_\infty^P \alpha = \int_\infty^P \beta = 0 \right\}$$

has size less than or equal to 3.

3.2. **Roots of p-adic power series.** Let $f'(t)$ be the local expansion of α (resp., β) in a residue disk, and let $f(t)$ be an antiderivative of $f'(t)$ whose constant term is either zero or the Coleman integral of α (resp., β) between ∞ and a $\mathbb{Q}_p$-rational point on C. To provably determine the roots of $f(t)$ lying in a residue disk up to a desired p-adic precision, we need to do the following:

- make sure that we truncate at a p-adic precision p^N that is able to detect all the roots (up to $O(p^n)$ where $n = N - k$, see Proposition 3.11);
- determine M such that to compute a root up to $O(p^n)$, we only need to consider the power series up to $O(t^M)$ where the coefficient of t^i is in $O(p^n)$ for all $i \geq M$ if the roots are simple and f is suitably normalized (i.e. $f \in \mathbb{Z}_p[[t]] \setminus p\mathbb{Z}_p[[t]]$).

Write $f(t) = f_M(t) + O(t^M)$ where M is an integer greater than or equal to $m_f + 2$ and $f_M(t)$ is a polynomial of degree less than or equal to $M - 1$. Then $f(t)$ and $f_M(t)$ have the same number of roots in $\mathbb{C}_p$ of p-adic valuation greater than or equal to 1, as can be deduced from the same considerations on the Newton polygon of $f(t)$ which imply Lemma 3.1 (for more details, see the proof of [MP12, Lemma 5.1]). We are interested in the zeros of $f(pt)$ in $\mathbb{Z}_p$. Note that

$$f(pt) - f_M(pt) \in O(p^n, t^M) \text{ for some } n \geq M.$$

Hence, $f(pt)$ and $f_M(pt)$ as polynomials in $\mathbb{Z}/p^n\mathbb{Z}$ have exactly the same zeros (including multiplicities). Furthermore, if a zero of $f(pt)$ (and $f_M(pt)$) modulo p^n is simple, then it lifts to a root of $f(pt)$ in $\mathbb{Z}_p$ by an inductive application of Hensel's lemma.

To compute a suitable choice of M, we require two more lemmas.

Lemma 3.9. *Let $\omega_i = (x^i/2y)dx$ for some $i \in \{0,1,2\}$, and $\lambda_i = \int_\infty^{P_0} \omega_i$. If $\overline{[P_0 - \infty]} \in \overline{J}(\mathbb{F}_p)$ has order prime to p, then $ord_p(\lambda_i) \geq 1$. In particular, this holds if p is a prime of non-anomalous reduction for J.*

Proof. Let n be the order of the reduction of $[P_0 - \infty]$ modulo p. Then $Q = n[P_0 - \infty] \in J_1(\mathbb{Q}_p)$, the kernel of reduction at p, and we have $\int_\infty^{P_0} \omega_i = \frac{1}{n}\int_0^Q \omega_{J,i}$, where $\iota^*(\omega_{J,i}) = \omega_i$. Now $\int_0^Q \omega_{J,i}$ can be computed by writing $\omega_{J,i}$ as a power series in $\mathbb{Z}_p[[z_1, z_2, z_3]]$ where z_1, z_2, z_3 is a local coordinate system for $J_1(\mathbb{Q}_p)$ around 0, formally integrating and evaluating at $z_1(Q), z_2(Q), z_3(Q)$. □

Lemma 3.10. *We have $f(pt) = \sum_{i=0}^\infty b_i t^i = \sum_{j=0}^\infty \frac{a_j p^{j+1}}{j+1} t^{j+1} + c$, where $c \in \mathbb{Q}_p$, $a_j \in \mathbb{Z}_p$ for all $j \geq 0$. Therefore for all $i \geq 1$, $ord_p(b_i) \geq i - ord_p(i)$. Furthermore if $p^2 \nmid \#J(\mathbb{F}_p)$ then $c \in \mathbb{Z}_p$.*

Proof. The first assertion is clear. For the latter, recall that c is either 0 or of the form $\int_\infty^Q \gamma$, for some $Q \in C(\mathbb{Q}_p)$ and $\gamma \in \{\alpha, \beta\}$. The proof is then similar to Lemma 3.9. □

By Lemma 3.10, we know that $f(pt)$ has coefficients in $\mathbb{Z}_p$, except possibly when $p^2 | \#J(\mathbb{F}_p)$. Let k be the minimum of the valuations of the coefficients of $f(pt)$. Note that, since $f'(t)$ mod p has order of vanishing equal to m_f, if $m_f < p-2$, it follows that the valuation of the coefficient of t^{m_f+1} in $f(pt)$ is precisely $m_f + 1$. Therefore $k \leq m_f + 1$. Furthermore, for $i > m_f + 1$, we have $\mathrm{ord}_p(b_i) \geq i - \mathrm{ord}_p(i) > i - (i - m_f - 1) = m_f + 1$.

Proposition 3.11. *Let $f(t)$ be an antiderivative of α or β, let $m_f < p-2$, and let k be the minimal valuation of the coefficients of $f(pt)$. Fix an integer N such that $m_f+2 \leq N \leq p^p - p$. Let ap^e be the smallest integer greater than or equal to N with $p \nmid a$ and $e \geq 1$, and set*

$$M = \begin{cases} ap^e + 1 & \text{if } ap^e - e < N, \\ N & \text{else.} \end{cases}$$

Then each simple root of $f_M(pt)$ in $\mathbb{Z}/p^{N-k}\mathbb{Z}$ equals the approximation modulo p^{N-k} of a root of $f(pt)$. Furthermore, if all such roots are simple, then these are all the roots of $f(pt)$ in $\mathbb{Z}_p$.

Proof. It suffices to show that for $i \geq M$, $\mathrm{ord}_p(b_i) \geq N$. Since $M \geq N$, the statement is clear for $p \nmid i$ by Lemma 3.10. Now suppose $p | i$ for some $i \geq M$. Hence, $i = bp^r$ where $p \nmid b$ and $r \geq 1$, and $bp^r \geq M \geq N$. Then by the definition of ap^e, we know that

$$bp^r \geq ap^e \quad \text{and} \quad 0 \leq ap^e - N < p.$$

We now have two cases to consider:

Case 1: Assume that $bp^r = ap^e$. It follows that $M = N = bp^r$ which in turn implies that $ap^e - e \geq N$. Then since $(a, e) = (b, r)$, we have that

$$\mathrm{ord}_p(b_i) \geq bp^r - r \geq N.$$

Case 2: Assume that $bp^r > ap^e$. It follows that $bp^r - ap^e \geq p$. Thus

$$\mathrm{ord}_p(b_i) \geq bp^r - r = (bp^r - ap^e) + (ap^e - r).$$

So if $\mathrm{ord}_p(b_i) < N$ then $r > (bp^r - ap^e) + (ap^e - N) \geq p$ and hence $p^p - p \leq bp^r - r < N$, contradicting our assumption on N. □

Remark 3.12. In order to apply Proposition 3.11 we need to meet the condition $m_f < p-2$; assuming that $p > 2g$ guarantees that this is always the case, as a consequence of the Riemann-Roch Theorem (see Remark 3.2). Furthermore, in the case when $p > 2g$, the hypothesis on N of Proposition 3.11 is always met, since $m_f + 2 < p < p^p - p$.

3.3. **Outline of the algorithm.** We retain the notation of the beginning of Section 3. The algorithm will always work if $p \geq 7$ and may or may not work if $p = 3$ or 5 (see Remark 3.2 and the comments in the main steps of the algorithm below). We now list the input and output of our algorithm followed by its main steps.

Input:

- C: a hyperelliptic curve of genus 3 over $\mathbb{Q}$ given by a model $y^2 = F(x)$ where $F \in \mathbb{Q}[x]$ is monic of degree 7, such that its Jacobian J has rank 1;
- p: an odd prime of good reduction for C not dividing the leading coefficient of F and $p \geq 7$;
- P_0: a point in $C(\mathbb{Q})$ such that $[P_0 - \infty] \in J(\mathbb{Q})$ has infinite order;
- $C(\mathbb{Q})_{\mathrm{known}}$: a list of all known rational points on $C(\mathbb{Q})$;
- the p-adic precision N (by Proposition 3.11, $N = 2p + 4$ is sufficiently large);
- the t-adic precision M (if $N = 2p + 4$ by Proposition 3.11, we can set $M = 2p + 1$).

Output: The set $Z \subseteq C(\mathbb{Q}_p)$ defined in (2.1) modulo the action of the hyperelliptic involution. In our code, this set is split into the following:

- a list of points of Z which can be recognized as points in $C(\mathbb{Q}) \setminus C(\mathbb{Q})_{\mathrm{known}}$ up to the hyperelliptic involution;
- a list of points $P \in Z$ such that $[P - \infty] \in J(\mathbb{Q}_p)_{\mathrm{tors}}$, up to the hyperelliptic involution (here, if P is not 2-torsion and is the localization of a point defined over a quadratic extension of $K/\mathbb{Q}$ then the coordinates in K are given as the corresponding minimal polynomials over $\mathbb{Q}$);
- a list of all remaining points $P \in Z$ (as above, if P is the localization of a point defined over a quadratic extension of $K/\mathbb{Q}$ then the coordinates in K are given as the corresponding minimal polynomials over $\mathbb{Q}$).

Main steps of the algorithm:

(1) *A basis for the annihilator.*
For each basis differential $\omega_i = (x^i/2y)dx$ $(i = 0, 1, 2)$, compute

$$\lambda_i = \int_\infty^{P_0} \omega_i \quad \text{modulo } p^n,$$

where n is the given p-adic precision. Set $k_{ij} := \min\{\mathrm{ord}_p(\lambda_i), \mathrm{ord}_p(\lambda_j)\}$ and

$$(\alpha, \beta) = \begin{cases} \left(\omega_0,\ p^{-k_{12}}(\lambda_1\omega_2 - \lambda_2\omega_1)\right) & \text{if } \lambda_0 = 0, \\ \left(p^{-k_{01}}(\lambda_0\omega_1 - \lambda_1\omega_0),\ p^{-k_{02}}(\lambda_0\omega_2 - \lambda_2\omega_0)\right) & \text{else.} \end{cases}$$

In either case, α and β are reductions modulo $p^{n'}$ of the pullback ι^* of a basis for the annihilator of $J(\mathbb{Q})$, where

$$n' = \begin{cases} n - k_{12} & \text{if } \lambda_0 = 0, \\ n - \max\{k_{01}, k_{02}\} & \text{else.} \end{cases}$$

By Lemma 3.9, $n' \leq n-1$ if p is non-anomalous. If $n' \geq 6$ we are guaranteed to be able to carry out all computations in the next steps when $p \geq 7$.

(2) *Ruling out residue disks.* Observe that we only need to consider residue disks up to the hyperelliptic involution.

Reduce α and β modulo p. For each $\overline{P} \in \overline{C}(\mathbb{F}_p)$, expand α and β in a local coordinate s around $\overline{P}$, calculate the orders of vanishing of α and β at $s = 0$, and let $m(\overline{P})$ denote their minimum. Note that $m(\overline{P}) \leq 2$ by Lemmas 3.3, 3.5 and 3.7, and hence it suffices to compute $\alpha(s)$ and $\beta(s)$ up to $O(s^2)$ to find $m(\overline{P})$.

If $m(\overline{P}) + 1$ equals the number of $\mathbb{Q}$-rational points in $C(\mathbb{Q})_{\text{known}}$ reducing to $\overline{P}$ modulo p and $m(\overline{P}) < p - 2$, then by Lemma 3.1 the set $C(\mathbb{Q})_{\text{known}}$ contains all $\mathbb{Q}$-rational points in the residue disk of $\overline{P}$. Otherwise, proceed to the next step.

(3) *Searching for the remaining disks.*

If, for a given point $\overline{P} \in \overline{C}(\mathbb{F}_p)$, the number of $\mathbb{Q}$-rational points in $C(\mathbb{Q})_{\text{known}}$ reducing to $\overline{P}$ modulo p is strictly smaller that $m(\overline{P}) + 1$, then we need to compute the set of $\mathbb{Q}_p$-rational points P reducing to $\overline{P}$ such that $\int_Q^P \alpha = \int_Q^P \beta = 0$ for a (any) rational point Q. For computational convenience we distinguish between two cases:

(i) If there exists $P \in C(\mathbb{Q})_{\text{known}}$ reducing to $\overline{P}$, let t be a uniformizer at P. Then expand α and β in t and formally integrate to obtain two power series $f(t)$, $g(t)$, which parametrize the integrals of α and β between P and any other point in the residue disk.

(ii) If we do not know any $\mathbb{Q}$-rational point in the residue disk of $\overline{P}$, then we may assume that $\overline{P} \neq \overline{\infty}$ and hence write $\overline{P} = (\overline{x_0}, \overline{y_0})$. If $\overline{y_0} = 0$, let $P = (x_0, 0)$ where x_0 is the Hensel lift of $\overline{x_0}$ to a root of $f(x)$. Otherwise, if $\overline{P}$ is not a Weierstrass point, we take $P = (x_0, y_0)$ where x_0 is any lift to $\mathbb{Z}_p$ of $\overline{x_0}$ (the Teichmüller lift of $\overline{x_0}$ would be a particularly convenient choice for x_0) and y_0 is obtained from $\overline{y_0}$ using Hensel's Lemma on $y^2 = F(x_0)$. Let $\tilde{f}(t)$ and $\tilde{g}(t)$ be the integrals between P and any other point reducing to $\overline{P}$ in terms of a local parameter t at P. Then write $f(t) = \tilde{f}(t) + \int_\infty^P \alpha$ and $g(t) = \tilde{g}(t) + \int_\infty^P \beta$.

Recall that in (1), we have computed the coefficients of the ω_i in α and β modulo n'. To provably compute the set of common zeros to a desired precision, we require that one of f or g have only simple roots, except possibly at $t = 0$ (in practice, this has been the case for every curve that we have considered). To check this requirement, we compute their discriminants, which are correct up to the p-adic precision of the coefficients.

Upon normalizing so that $t = 0$ is not a root of either f or g, assume without loss of generality that f has only simple roots. The t-adic precision we should compute $f(t)$ to in order to find provably correct approximations of its simple zeros is determined by Proposition 3.11. In practice, we truncate $f(t)$ at $O(t^M)$ where $M = n'$, unless the smallest multiple r of p greater than or equal to n' satisfies $r - \text{ord}_p(r) < n'$, in

which case take $M = r + 1$. For the p-adic precision, the coefficients are computed modulo $p^{n'}$. Then the simple roots are correct up to $O(p^{n'-k})$ where k is the minimal valuation of the coefficients of $f(pt)$ (cf. the discussion preceding Proposition 3.11). To compute the roots we use the function `polrootspadic` implemented in `PARI/GP`. Finally, we take the list of roots which lie in $p\mathbb{Z}_p$ and check whether they are also roots of g.

If $p = 3$ or $p = 5$ and the order of vanishing of $f(t)$ or $g(t)$ modulo p is greater than or equal to $p - 2$, then we cannot provably find the zeros of $f(pt)$ and $g(pt)$. Currently the algorithm assumes that $p \geq 7$ to avoid these pitfalls.

(4) *Identifying the remaining classes.*

Once we have found the common zeros of $f(pt)$ and $g(pt)$, we recover the corresponding $\mathbb{Q}_p$-rational points that do not come from points in $C(\mathbb{Q})_{\text{known}}$. We now have the output set that we will now break into sublists.

If we fail to recognize a point Q as $\mathbb{Q}$-rational, we can check whether the integral between ∞ and Q of any non-zero differential γ not in the span of α and β also vanishes: if this is the case, the point $[Q - \infty] \in J(\mathbb{Q}_p)$ is torsion (cf. [Col85b, Proposition 3.1]) and if we know explicitly $J(\mathbb{Q})_{\text{tors}}$ (which in general is computable) we can verify whether Q is $\mathbb{Q}$-rational or not. Furthermore, by increasing the degree in `algdep`, we may even try to identify the number field over which the coordinates of Q are defined[1]. This may require high p-adic precision; however, it was possible for every curve we considered.

If the integral of the differential γ is non-zero, and we have not recognized Q as a $\mathbb{Q}$-rational point, we can still check whether the point Q is defined over some number field K. For instance $[Q - \infty]$ could equal a point in $J(\mathbb{Q})$ plus some torsion element in $J(K)$, with $[K : \mathbb{Q}] > 1$ (see Example 4.1).

3.4. **Generalizations of the algorithm.**

3.4.1. *What if we do not know $P_0 \in C(\mathbb{Q})$ such that $[P_0 - \infty] \notin J(\mathbb{Q})_{\text{tors}}$?*

The hyperelliptic curve we input in the algorithm is assumed to have rank 1. Calculation of the rank is attempted by `Magma` [BCP97] by working out both an upper bound and a lower bound, the former coming from computation of the 2-Selmer group and the latter from an explicit search for linearly independent points on the Jacobian. The success of the rank computation relies on the two bounds being equal. In particular, if we suppose that we know provably that the rank of the Jacobian is one, we may as well assume that we know a point $Q \in J(\mathbb{Q})$ of infinite order and a divisor E on C representing it. Then we may proceed as follows. The first task is to write $Q = [E]$ in the form $[D - d\infty]$, where D is an effective $\mathbb{Q}$-rational divisor. In order to achieve this, we follow step by step the proof of [Sto14, Corollary 4.14]. That is, we compute the dimension of $(E + n\infty)$ for $n = 0, 1, 2, \ldots$ (here $(E + n\infty)$ denotes the Riemann-Roch space of $E + n\infty$), until we find the smallest $n = m$ for which the dimension is 1. Then $D - d\infty = E + \text{div}(\phi)$, where ϕ generates $(E + m\infty)$. By [Sto14, Lemma 4.17], D is then the unique $\mathbb{Q}$-rational divisor in general position and of degree less than or equal to $g = 3$ such that Q can be represented in the form $[D - d\infty]$.

[1]The hyperelliptic curve C is defined over $\mathbb{Q}$. Thus the fact that $[Q - \infty] \in J(\mathbb{Q}_p)_{\text{tors}}$ forces Q to have coordinates in $\overline{\mathbb{Q}} \cap \mathbb{Q}_p$.

Let K be the smallest Galois extension of $\mathbb{Q}$ over which the support of D is defined. Furthermore, let p be a prime of good reduction for C that splits completely in $K/\mathbb{Q}$ (there are infinitely many such primes). Then K can be realized as a subfield of $\mathbb{Q}_p$ and hence the support of D can be seen as lying in $C(\mathbb{Q}_p)$. Write $D = \sum_{i=1}^{d} P_i$ (some P_i possibly being equal). Then we may proceed exactly as before, just replacing λ_i in (1) by

$$\lambda_i = \sum_{i=1}^{d} \int_{\infty}^{P_i} \omega_i.$$

3.4.2. *Even degree model.* The algorithm relies heavily on computations of Coleman integrals, for which one needs the hyperelliptic curve considered to have a model of the form $y^2 = F(x)$, where $F(x)$ is monic. In particular, if one were to work with an even degree model, the two points at infinity would necessarily be defined over $\mathbb{Q}$ [Sto14]. Therefore we could proceed as in the odd degree case with the single point at infinity being replaced by one of these two points. If $F(x)$ is not monic, the issue is that Coleman integration is not implemented in `Sage`, though an implementation is available in `Magma` [BT17, BT]. Hence, general even models could be handled by computing the set of local points Z as defined in (2.1), using the sum of the two points at infinity as the divisor D.

3.4.3. *Other ranks and genera.* Our assumptions on g and r are somewhat arbitrary. With minor modifications, our code can be used in more general cases, provided that $0 < r < g$.

4. Curve Analysis

Once we implemented in `Sage` the algorithm described in the previous section, we ran it over $16,977$ hyperelliptic curves of genus $g = 3$ satisfying the following properties:

(1) the curve admits an odd degree model over $\mathbb{Q}$;
(2) the Jacobian of the curve has Mordell–Weil rank equal to 1;
(3) there is a $\mathbb{Q}$-rational point P_0 such that $[P_0 - \infty]$ has infinite order in $J(\mathbb{Q})$.

In order to obtain those curves, we sorted the $67,879$ genus 3 hyperelliptic curves from a forthcoming database of genus 3 curves over $\mathbb{Q}$ [BPSS]. Out of these, $19,254$ curves satisfy conditions (1) and (2).

Running our code for the $16,977$ curves for which we could further find a P_0 as in (3), we found 75 curves where the zero set Z contains something other than the rational points we had already computed and Weierstrass points defined over $\mathbb{Q}_p$ for our chosen prime p. Note that in all $16,977$ computations, the prime p used was the smallest prime greater than $2g = 6$ which divided neither the discriminant nor the leading coefficient of the hyperelliptic polynomial defining the curve.

Let C be one of these 75 curves, let W denote the set of Weierstrass points in $C(\mathbb{Q}_p) \setminus C(\mathbb{Q})$ and let $P \in Z \setminus (C(\mathbb{Q}) \cup W)$. In all cases, we identified P as a point defined over a quadratic extension K of $\mathbb{Q}$ in which p splits. Even so, these 75 curves split up into 3 distinct cases:

(1) $[P - \infty] \in J(K)_{\text{tors}}$;
(2) $[P - \infty] \notin J(K)_{\text{tors}}$ but $n[P - \infty] \in J(\mathbb{Q})$ for some positive integer n;
(3) $\langle J(\mathbb{Q}), [P - \infty] \rangle_{\mathbb{Z}}$ is a rank 2 subgroup of $J(K)$.

In cases (1) and (2), it is clear why $P \in Z$. On the other hand, justifying case (3) requires investigating more closely the geometry of the Jacobian of the curve, as is carried out in detail in Example 4.3.

4.1. **Examples.** For each of the curves below we give a list of known rational points, which are all of the rational points up to a height[2] of 10^5. Following the algorithm outlined in §3.3, we produce the set Z of local points for the prime $p = 7$ or $p = 11$, which in each case returns no new $\mathbb{Q}$-rational points, hence concluding that the set of known rational points $C(\mathbb{Q})_{\text{known}}$ is all of $C(\mathbb{Q})$. In each of the examples below, however, Z contains a $\mathbb{Q}_p$-point which is not a Weierstrass point and falls into one of the cases outlined above.

Example 4.1. Consider the hyperelliptic curve

$$y^2 + x^3y = x^7 + 2x^6 - 2x^5 - 9x^4 - 4x^3 + 8x^2 + 8x + 2$$

(given above by a minimal model) which has absolute minimal discriminant 544256 and whose Jacobian has conductor $544256 = 2^9 \cdot 1063$. We work with an odd degree model

$$C : y^2 = 4x^7 + 9x^6 - 8x^5 - 36x^4 - 16x^3 + 32x^2 + 32x + 8,$$

which has the following five known rational points:

$$C(\mathbb{Q})_{\text{known}} = \{\infty, (-1,-1), (-1,1), (1,-5), (1,5)\}.$$

Running the code on C together with the prime $p = 7$ and the point $P_0 = (-1,-1)$, we find that

$$Z = C(\mathbb{Q})_{\text{known}} \cup W \cup \{(0, \pm 2\sqrt{2})\},$$

where the set W of non-$\mathbb{Q}$-rational Weierstrass points has size 3. Moreover, the points $[(0, \pm 2\sqrt{2}) - \infty] \in J(\mathbb{Q}(\sqrt{2}))$ have order 12.

Example 4.2. Consider the hyperelliptic curve

$$y^2 + (x^4 + 1)y = 2x^3 + 2x^2 + x$$

(given above by a minimal model) which has absolute minimal discriminant 48519 and whose Jacobian J has conductor $48519 = 3^4 \cdot 599$. We work with an odd degree model

$$C : y^2 = -4x^7 + 24x^6 - 56x^5 + 72x^4 - 56x^3 + 28x^2 - 8x + 1.$$

This curve has the following five known rational points:

$$C(\mathbb{Q})_{\text{known}} = \{\infty, (0,-1), (0,1), (1,-1), (1,1)\}.$$

[2] Our computations show that the $\mathbb{Q}$-rational points of highest absolute logarithmic height (with respect to an odd degree model) on a curve among the 16,977 hyperelliptic curves that we considered, are

$$\left(-\frac{49}{18}, -\frac{339563}{11664}\right), \left(-\frac{49}{18}, -\frac{1600445}{52488}\right)$$

on the hyperelliptic curve

$$C : y^2 + (x^4 + x^2 + x)y = x^7 - x^6 - 5x^5 + 5x^3 - 3x^2 - x,$$

which has absolute minimal discriminant 5326597 and whose Jacobian has conductor 5326597.

For this example we will give a more detailed outline of the algorithm. Following Section 2.1 we know that there exist functions $\lambda_{\alpha,\infty}$, $\lambda_{\beta,\infty}$ on $C(\mathbb{Q}_p)$, corresponding to differentials $\alpha, \beta \in H^0(C_{\mathbb{Q}_p}, \Omega^1)$. These two functions vanish on the rational points of C, i.e.,

$$C(\mathbb{Q}) \subseteq \ker(\lambda_{\alpha,\infty}) \cap \ker(\lambda_{\beta,\infty}) = Z.$$

We would like to know whether this zero set Z contains anything other than the $\mathbb{Q}$-rational points on C.

If we take $p = 11$, we find that $Z = C(\mathbb{Q})$. Observe that 11 is inert in $K = \mathbb{Q}(\sqrt{-3})$.

If we take $p = 7$, which splits in $K = \mathbb{Q}(\sqrt{-3})$, we find that there are four points defined over $K = \mathbb{Q}(\sqrt{-3})$ that appear in Z. Up to hyperelliptic involution, we have

$$\left\{\left((1+\sqrt{-3})/2, \sqrt{-3}\right), \left((1-\sqrt{-3})/2, \sqrt{-3}\right)\right\} \subseteq Z.$$

There is a good reason for the presence of these points in Z: if P denotes any of the above points, then $5[P - \infty] \in J(\mathbb{Q})$, therefore $5\lambda_\alpha(P) = 0$.

We now run through the algorithm to see that for $p = 7$ we find that

$$C(\mathbb{Q})_{\text{known}} \cup \left\{\left((1+\sqrt{-3})/2, \sqrt{-3}\right), \left((1-\sqrt{-3})/2, \sqrt{-3}\right)\right\} = Z \quad \text{up to hyperelliptic involution.}$$

First we change variables to obtain an equation for C where the defining polynomial $F(x)$ is monic, so we send $x \mapsto -4x$, $y \mapsto 4^4 y$. The $\mathbb{F}_7$-points of C are

$$C(\mathbb{F}_7) = \{\overline{\infty}, \overline{(0,2)}, \overline{(0,5)}, \overline{(1,4)}, \overline{(1,3)}, \overline{(2,4)}, \overline{(2,3)}, \overline{(4,4)}, \overline{(4,3)}, \overline{(5,2)}, \overline{(5,5)}\}.$$

Of these eleven points, five of them arise as reductions of known $\mathbb{Q}$-rational points, and an order of vanishing calculation shows that these are the only rational points in those residue disks. For the remaining six $\mathbb{F}_7$-points of C, the same order of vanishing calculation shows that there is at most one $\mathbb{Q}_p$-point in each residue disk corresponding to these points on which $\lambda_{\alpha,\infty}$ and $\lambda_{\beta,\infty}$ vanish.

We know that the four quadratic points above reduce to

$$\{\overline{(1,4)}, \overline{(1,3)}, \overline{(4,4)}, \overline{(4,3)}\}$$

in some order (note that the quadratic points listed above are on the original curve, and these $\mathbb{F}_7$-points are the images after the change of variables of their reductions). Hence, our task is now reduced to the analysis of the residue disks of $\overline{(2,4)}$ and $\overline{(2,3)}$, which moreover map to each other under the hyperelliptic involution. To show that $\lambda_\alpha, \lambda_\beta$ have no zeros in these residue disks, we will explicitly write down the power series and compute their zeros using `PARI/GP`, as outlined in §2.1.

As usual, let $\omega_i = x^i/2y$. Then the annihilator of $J(\mathbb{Q})$ under the integration pairing is spanned by

$$\begin{aligned}
\alpha &= (1 + 2\cdot 7 + 7^2 + 2\cdot 7^3 + 5\cdot 7^4 + O(7^5))\,\omega_0 + (4 + 7^2 + 5\cdot 7^4 + O(7^5))\,\omega_1, \\
\beta &= (6 + 3\cdot 7 + 2\cdot 7^2 + 5\cdot 7^4 + O(7^5))\,\omega_0 + (4 + 7^2 + 5\cdot 7^4 + O(7^6))\,\omega_2.
\end{aligned}$$

It suffices to consider the residue disk of $\overline{(2,4)}$. In this residue disk, we obtain the two power series

$$\begin{aligned}
f(t) &= 2\cdot 7 + 4\cdot 7^2 + O(7^3) + (2 + 7 + 2\cdot 7^2 + O(7^3))t + (6 + 5\cdot 7 + 4\cdot 7^2 + O(7^3))t^2 + \cdots, \\
g(t) &= 7 + 6\cdot 7^2 + O(7^3) + (1 + 5\cdot 7 + 2\cdot 7^2 + O(7^3))t + (3 + 4\cdot 7 + 7^2 + O(7^3))t^2 + \cdots.
\end{aligned}$$

Each of these have one zero in $p\mathbb{Z}_p$, but not the same zero. The two zeros are $6\cdot 7+5\cdot 7^2+O(7^3)$ and $6\cdot 7+2\cdot 7^2+O(7^3)$, respectively.

Example 4.3. Consider the hyperelliptic curve

$$y^2+(x^3+x)y = x^7-4x^6+8x^5-10x^4+8x^3-4x^2+x,$$

(given above by a minimal model) which has absolute minimal discriminant 1573040 and whose Jacobian J has conductor $786520 = 2^3\cdot 5\cdot 7\cdot 53^2$. We work with the odd degree model

$$C : y^2 = 4x^7-15x^6+32x^5-38x^4+32x^3-15x^2+4x,$$

on which we know the following rational points:

$$C(\mathbb{Q})_{\text{known}} = \{\infty, (0,0), (1,-2), (1,2)\}.$$

The point $R = [(1,-2)-\infty]$ has infinite order in $J(\mathbb{Q})$ and can thus be used to initiate the algorithm of §3.3 with $p = 11$, which is the smallest prime greater than 6 of good reduction for C. We find that

$$Z = C(\mathbb{Q})_{\text{known}} \cup W \cup \{(-1, \pm 2\sqrt{-35})\},$$

where W has size 2. In particular, we have $C(\mathbb{Q}) = C(\mathbb{Q})_{\text{known}}$.

Perhaps more interestingly, we now explain[3] why $\{(-1,\pm 2\sqrt{-35})\} \subseteq Z$. Let $K = \mathbb{Q}(\sqrt{-35})$, $\mathrm{Gal}(K/\mathbb{Q}) = \langle\tau\rangle$ and fix an embedding $K \to \mathbb{Q}_p$. The point

$$Q = [(-1, 2\sqrt{-35}) - \infty] \in J(K)$$

is of infinite order, as there exists a non-zero differential in $H^0(J_{\mathbb{Q}_p}, \Omega^1)$ whose integral does not vanish on Q. Suppose that $nQ \in J(\mathbb{Q})$ for some integer $n \neq 0$. Then $nQ = (nQ)^\tau = nQ^\tau$ and hence $2Q = Q - Q^\tau \in J(K)_{\text{tors}}$, a contradiction. It follows that $J(\mathbb{Q})$ and Q generate a subgroup of rank 2 in $J(K)$. A computation in `Magma` shows that the rank of $J(K)$ itself is equal to 2. Therefore, the image of $Z \setminus W$ in $J(K)$ generates a subgroup of finite index. Showing that $(-1, \pm 2\sqrt{-35}) \in Z$ is then equivalent to proving that the dimension of the p-adic closure of $J(K)$ in $J(\mathbb{Q}_p)$ is 1, i.e. that the $\mathbb{Z}$-linear independence of Q and $J(\mathbb{Q})$ is not preserved under base-change to $\mathbb{Q}_p$.

To explain this phenomenon, we compute the automorphism group of C using `Magma`. We have that $\mathrm{Aut}(C) \cong C_2 \times C_2$, where the first copy of C_2 is generated by the hyperelliptic involution $i : C \to C$ and the second one is generated by $\phi : C \to C$, $\varphi(x,y,z) = (z,y,x)$. The quotient $C/\langle\phi\rangle$ is the elliptic curve

$$E : y^2+xy+y = x^3-x^2,$$

whereas the quotient $C/\langle\varphi\circ i\rangle$ is the genus 2 hyperelliptic curve

$$H : y^2+(x^2+1)y = x^5+x^4-4x^3+3x^2-x-1.$$

It follows that J decomposes, over $\mathbb{Q}$, as a product of E and the Jacobian of H, which is an abelian surface A with no extra endomorphisms [Pau08, Theorem 4] .

Since $\mathrm{rank}(E(\mathbb{Q})) = \mathrm{rank}(J(\mathbb{Q})) = 1$ and the p-adic closure of $E(L)$ in $J(\mathbb{Q}_p)$ can have dimension at most one for any number field L where p splits completely and any embedding

[3]We are grateful to Andrew Sutherland for kindly computing real endomorphism algebras (using the techniques of [BSS+16, HS16]) for a number of curves that produced Chabauty–Coleman output similar to this example, which greatly assisted in understanding the structure of their Jacobians. We would also like to thank Bjorn Poonen for a very helpful discussion about this phenomenon.

$L \to \mathbb{Q}_p$, in order to determine which points of $C(\overline{\mathbb{Q}})$ can appear in Z, we then need to search for points that map to torsion points in A, under the quotient map $C \to C/\langle \varphi \circ i \rangle \to A$.

An explicit computation using Coleman integrals on H shows that $H(\mathbb{Q}_p) \cap A(\mathbb{Q}_p)_{\text{tors}} \subseteq A(\mathbb{Q}_p)[2]$, where, as usual, the embedding of H into A is via the base-point ∞. Let $T = (x, y, z) \in C(\mathbb{Q}_p)$. Then $\varphi \circ i(T) = (z, -y, x)$: thus, T maps into $A(\mathbb{Q}_p)_{\text{tors}}$ iff either $T = (0, 0)$, $T = \infty$ or $(z, -y, x) = (x, -y, z)$, i.e. $x^2 = 1$. This shows both why $\{(-1, \pm 2\sqrt{-35})\} \subset Z$ and why no other non-torsion point in $C(\overline{\mathbb{Q}})$ can occur in Z besides $(1, \pm 2)$ and $(-1, \pm 2\sqrt{-35})$.

References

[Bal15] J. S. Balakrishnan, *Explicit p-adic methods for elliptic and hyperelliptic curves*, Advances on superelliptic curves and their applications, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., vol. 41, IOS, Amsterdam, 2015, pp. 260–285. MR 3525580 2.2.1, 3.1, 3.1

[BBCF+] J. S. Balakrishnan, F. Bianchi, V. Cantoral-Farfán, M. Çiperiani, and A. Etropolski, *Sage code*, https://github.com/jbalakrishnan/WIN4. 1

[BBK10] J. S. Balakrishnan, R. W. Bradshaw, and K. S. Kedlaya, *Explicit Coleman integration for hyperelliptic curves*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 6197, Springer, Berlin, 2010, pp. 16–31. MR 2721410 1, 2.2.2

[BCP97] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR MR1484478 3.4.1

[BPSS] A. Booker, D. Platt, J. Sijsling, and A. Sutherland, *Genus 3 hyperelliptic curves*, http://math.mit.edu/~drew/gce_genus3_hyperelliptic.txt. 1, 4

[BS08] N. Bruin and M. Stoll, *Deciding existence of rational points on curves: An experiment*, Experiment. Math. **17** (2008), no. 2, 181–189. 1

[BS10] ———, *The Mordell-Weil sieve: proving non-existence of rational points on curves*, LMS J. Comput. Math. **13** (2010), 272–306. MR 2685127 2

[BSS+16] A. R. Booker, J. Sijsling, A. V. Sutherland, J. Voight, and D. Yasaki, *A database of genus-2 curves over the rational numbers*, LMS J. Comput. Math. **19** (2016), no. suppl. A, 235–254. 3

[BT] J. S. Balakrishnan and J. Tuitman, *Magma code*, https://github.com/jtuitman/Coleman. 3.4.2

[BT17] ———, *Explicit Coleman integration for curves*, Arxiv preprint (2017). 3.4.2

[Cha41] C. Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, C.R. Acad. Sci. Paris **212** (1941), 882–885. 1, 2.1

[Col85a] R. F. Coleman, *Effective Chabauty*, Duke Math. J. **52** (1985), no. 3, 765–770. MR 808103 1, 2.2

[Col85b] ———, *Torsion points on curves and p-adic abelian integrals*, Ann. of Math. (2) **121** (1985), no. 1, 111–168. MR 782557 1, 2.2.2, 4

[Fal83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366. 1, 2.1

[HS16] D. Harvey and A. V. Sutherland, *Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time, II*, Frobenius distributions: Lang-Trotter and Sato-Tate conjectures, Contemp. Math., vol. 663, Amer. Math. Soc., Providence, RI, 2016, pp. 127–147. 3

[Kob84] N. Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, second ed., Graduate Texts in Mathematics, vol. 58, Springer-Verlag, New York, 1984. MR 754003 3.1, 3.1

[Maz77] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978). 1

[Mil86] J. S. Milne, *Jacobian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 167–212. MR 861976 2.1

[MP12] W. McCallum and B. Poonen, *The method of Chabauty and Coleman*, Explicit methods in number theory, Panor. Synthèses, vol. 36, Soc. Math. France, Paris, 2012, pp. 99–117. 3.1, 3.2, 3.2

[Pau08] J. Paulhus, *Decomposing Jacobians of curves with extra automorphisms*, Acta Arithmetica **132** (2008), no. 3, 231–244 (eng). 4.3

[S+17] W. A. Stein et al., *Sage Mathematics Software (Version 8.1)*, The Sage Development Team, 2017, http://www.sagemath.org. 1

[Sto14] M. Stoll, *Arithmetic of Hyperelliptic Curves*, 2014. 3.4.1, 3.4.2

[Wet97] J. L. Wetherell, *Bounding the number of rational points on certain curves of high rank*, ProQuest LLC, Ann Arbor, MI, 1997, Thesis (Ph.D.)–University of California, Berkeley. MR 2696280 2.1, 2.1, 2.2.1

Jennifer S. Balakrishnan, Department of Mathematics and Statistics, Boston University, 111 Cummington Mall, Boston, MA 02215, USA
E-mail address: jbala@bu.edu

Francesca Bianchi, Mathematical Institute, University of Oxford, Andrew Wiles Building, Radcliffe Observatory Quarter, Woodstock Road, Oxford OX2 6GG, UK
E-mail address: francesca.bianchi@maths.ox.ac.uk

Victoria Cantoral-Farfán, ICTP - 11 Strada Costeira, Trieste, Italy
E-mail address: vcantora@ictp.it

Mirela Çiperiani, Department of Mathematics, The University of Texas at Austin, 1 University Station, C1200 Austin, Texas 78712, USA
E-mail address: mirela@math.utexas.edu

Anastassia Etropolski, Department of Mathematics, Rice University MS 136, Houston, TX 77251, USA
E-mail address: aetropolski@rice.edu